thycotic®

IT Security That Works.

Warum „Privileged Account Management“ (PAM)?

Privilegierte Accounts wie z.B. der lokale- oder der Domänen Admin müssen kontrolliert werden, um die Integrität des Netzwerks zu erhalten. Diese Accounts werden verwendet, um Daten im Netzwerk freizugeben, Software zu installieren und auszuführen, kritische Netzwerkgeräte zu verwalten und das Netzwerk vor internen und externen Bedrohungen zu schützen. Privilegierte Accounts sind eine ideale Zielscheibe für Angriffe und können zu einem Sicherheitsproblem für jede Organisation werden.

58% aller Vorfälle in der IT-Sicherheit werden durch interne Bedrohungen verursacht.

- InfoSecurity Magazin

21% der Unternehmen glauben, derzeitige und ehemalige Mitarbeiter stellen die größte Gefahr für die Cybersecurity dar.

- US State of Cybercrime Survey

Das Dashboard von Secret Server bietet eine anpassbare Konsole, um die privilegierten Accounts zu verwalten.

Die Lösung: Secret Server

Secret Server hilft Ihrem Unternehmen einen kritischen Teil der IT-Infrastruktur, die privilegierten Accounts, zu verwalten. IT-Teams benötigen ein bewährtes Tool um die Netzwerk-Sicherheit innerhalb der Organisation zu gewährleisten und die „Business Continuity“ zu garantieren.

Benutzen Sie Secret Server für:

- **Risikoreduzierung.** Die Durchsetzung von Passwortrichtlinien, die Kontrolle vertraulicher Anmeldeinformationen, und ein automatisierte Passwortwechsel schützen Ihr Unternehmen vor Angriffen. Die Integration mit ergänzenden IT-Sicherheitstools (2-Faktor-Authentifizierung, Schwachstellen-Management, SIEM) bietet Ihnen einen ganzheitlichen Netzwerksicherheitsansatz.
- **Compliance.** Auditoren prüfen, ob Ihre privilegierten Accounts geschützt sind. In diesem Zug bietet Thycotic Secret Server eine Vielzahl an Berichten zur Überwachung der einzelnen Accounts (Wer macht was, wann, wo und wie?). Des Weiteren hilft Thycotic folgende Compliance-Anforderungen zu erfüllen: PCI-DSS, HIPAA, SOX, FISMA, Basel 2 und viele mehr.
- **Mehr Effizienz durch höhere Netzwerksicherheit.** Das Verwalten von privilegierten Accounts ist komplex und zeitaufwendig für Ihre IT. Automatisierte Passwortwechsel erhöhen die Produktivität ihrer Administratoren und sorgen dafür, dass ihr Netzwerk zu jeder Zeit gesichert ist.

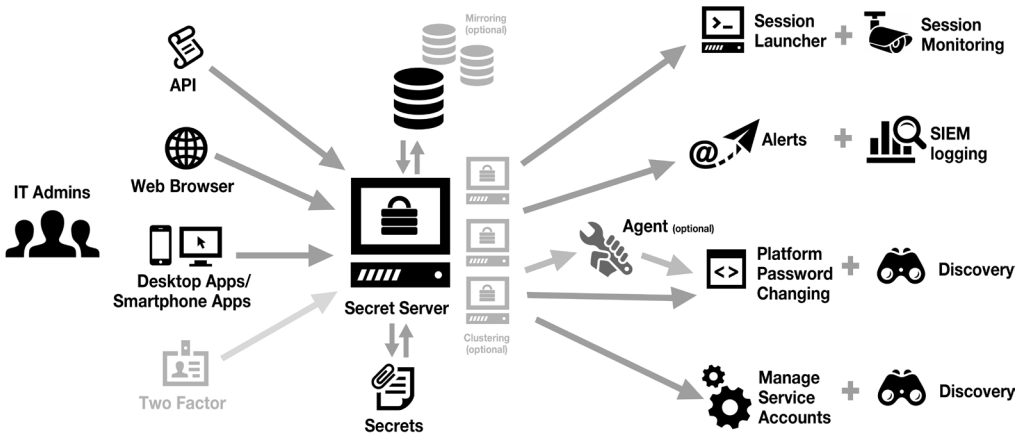
Warum Secret Server?

Secret Server liefert Ihnen umgehend Mehrwert durch erhöhte Netzwerksicherheit und Kosten sparende automatisierte Prozesse.

Ihre Vorteile

- Intuitive Installation und Administrationsoberfläche
- Zuverlässige Architektur
- Umfassende technische Unterstützung und Dokumentation

Secret Server®



Vorteile von Secret Server

- **Minimierung der Bedrohungen von Innen.** Sperren Sie einzelne Zugänge, so dass gewährleistet ist, dass Mitarbeiter nur auf die Bereiche Zugriff haben, die sie auch brauchen. Zusätzlich können Kontrollmechanismen angepasst werden, um Sicherheitsrichtlinien zu erfüllen.
- **Schützen Sie ihre Daten und Ihr Netzwerk vor externen Bedrohungen** wie z.B. Advanced-Persistent Threat (APT), phishing, password cracking, pass the hash, social engineering, Denial of Service (DoS), SQL-Injection und vielem mehr.
- **Compliance-Anforderungen**
  Seien Sie sich sicher bei der Erfüllung von Compliance Vorgaben für Passwortsicherheit und Zugangskontrolle.
- **Erhöhen Sie die Effizienz ihrer Mitarbeiter**
  Manuelle Passwortänderung ist ein äußerst zeitaufwendiger Prozess. Gewinnen Sie aktiv Arbeitszeit zurück durch voll automatisierte Prozesse.
- **Vermeiden Sie Netzwerkausfälle**
  Fehlerhafte oder verlorene Passwörter verursachen Netzwerkausfälle, Verzögerungen beim Wiederherstellen der Passwörter für Produktionssysteme, bis hin zu kostspieligen Ausfällen und der Beeinträchtigung des Vertrauens Ihrer Kunden in Ihre IT.
- **Überwachung der Netzwerkzugriffe**
  Erhalten Sie Echtzeitüberwachung über die Aktivität aller privilegierten Accounts in der gesamten Infrastruktur für mehr Visibilität.
- **Verantwortlichkeit stärken**
  Definieren Sie Rechte und Zuständigkeiten, erfassen Sie die Aktivität von administrativen Benutzern und erhalten Sie volle Transparenz und Nachvollziehbarkeit aller Zugriffe.
- **Beseitigung von unzulänglichem Password-Management**
  Wie z.B. Freeware Tools oder Excel-Tabellen, auf die jeder Zugriff hat. Gehen Sie nicht davon aus dass die richtigen Tools/Verfahren in ihrer Firma vorhanden sind um privilegierte Accounts richtig zu verwalten.

Kontrollieren Sie ihre privilegierten Accounts mit Secret Server

Unterstützte Plattformen

- Windows Local Admin Accounts
- Unix/Linux/Mac
- SAP
- Oracle
- Sybase
- Cisco
- Juniper
- Cloud - AWS, Google, Azure
- AS/400
- MS SQL Server
- MySQL
- Firewalls
- Storage Systeme
- Und mehr

Web-based centralized management

- Import & Export
- Rollenbasierte Zugriffskontrolle (RBAC)
- Ordner mit interaktiver Suche

Service account managment

- Windows Dienste
- Scheduled Tasks
- COM+
- Application Pools (IIS, asp.net)
- Flat Files
- PowerShell

Integrationen

- Active Directory/LDAP
- SIEM
- HSM
- RADIUS (TFA)
- Schwachstellen-Management
- Vulnerability Scanning
- Und weitere

Auditierung

- Vollständiges Reporting
- Anpassbare Alarme
- Aufzeichnung von Sitzungen

Disaster Recovery

- Automatisierte Backups
- Klartext Export
- “Unlimited admin” Notfall Vollzugriff
- Datenbank Spiegelung
- Hochverfügbarkeit

Advanced security features

- Check Out (Einmalpasswort)
- “DoubleLock” Zusätzliche Verschlüsselung für sensible Daten
- “Approval work flow” Genehmigungs-WorkFlow
- FIPS 140-2
- IP Restriktionen

thycotic

partner@thycotic.com

p: +1 202-802-9399
t: @thycotic
www.thycotic.com